

REMARKS

Claims 1-5, 11-19, 21-24, 26-30, 32-57, 59-63, 85-87, 89-92, 98-106, 108-110, 112-116, 118-127, 128-133 and 155-157, 160-183 are pending in the present application. Claims 29, 85, 115, 155, and 180 are amended above. No new matter is added by the claim amendments. Entry is respectfully requested.

Claims 1-5, 11-14, 20, 25, 26, 89-92, 98-101, 107, 111, 112, 184, 185, 189 and 190 stand rejected under 35 U.S.C. 102(e) as being anticipated by Reitmeier, *et al.* (U.S. Publication Number 2002/0003881). The applicants note that claims 20, 25, 107 and 111 were cancelled by Applicant in Amendment B filed June 7, 2007. Claims 15-19, 21-24, 102-106 and 108-109 and 100 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* (U.S. Patent Number 5,930,828). The applicants note that although the remarks in the Office Action indicate that claim 100 rather than claim 110 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.*, the applicants assume that claim 110 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* Claims 27, 28, 113 and 114 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* (U.S. Publication Number 2006/0053307). Claims 29, 30, 32-39, 43-53, 85-87, 115, 116, 118-121, 123-125, 155-157, 161-166, 180-183 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* Claims 40, 41, 42 and 122 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Weidong (U.S. Patent Number 6,819,766). Claims 54 and 55 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Xu, *et al.* Claims 56, 57, 59-63, 126, 127, 129, 130, 132, 133, 167-171, 175 and 176 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* Claims 172-174 and 177-179 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Jensen, *et al.* Claims 131 and 61 stand rejected under 35 U.S.C. 103(a) as being

unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Atallah, *et al.* (U.S. Publication Number 2006/0031686). Claims 186, 187, 188, 191, 192 and 193 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Wiedong. Reconsideration of the rejections and allowance of the claims are respectfully requested.

In the present invention as claimed in independent claims 1, 161 and 167, a method of preventing unauthorized use of digital content data includes subdividing the digital content data into data segments and modifying the data segments with second data to generate modified data. Modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data. The method further includes storing the modified data at predetermined memory locations. The method further includes retrieving the modified data from the predetermined memory locations and, following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments.

In the present invention as claimed in independent claim 29, a method of preventing unauthorized use of digital content data in a system having memory locations includes subdividing the digital content data into data segments and modifying the data segments with second data to generate modified data. The method further includes scanning the system to determine available memory locations, selecting target memory locations with the available memory locations at which to store the modified data and storing the modified data at the target memory locations. A subset of the available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located.

In the present invention as claimed in independent claim 56, a method for preventing unauthorized use of digital content data hosted on a system includes modifying digital content data to generate modified data. The method further includes determining whether an unauthorized attempt at accessing the digital content data occurs and, in the event of

unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter the unauthorized activity.

In the present invention as claimed in independent claim 85, a method for preventing unauthorized use of digital content data in a system having memory locations includes scanning the system to determine available memory locations, selecting target memory locations within the available memory locations and storing the digital content data at the target memory locations. A subset of the available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located.

In the present invention as claimed in independent claims 89 and 175, a system for preventing unauthorized use of digital content data includes a subdividing unit for subdividing the digital content data into data segments, a modification unit for modifying the data segments with second data to generate modified data. Modifying the data segments includes interleaving the data segments with the second data to generate interleaved data. The system further includes a storage unit for storing the modified data at predetermined memory locations. The system further includes a means for retrieving the modified data from the predetermined memory locations and a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original digital content data.

In the present invention as claimed in independent claim 115, a system for preventing unauthorized use of digital content data in a system having memory locations includes a means for subdividing the digital content data into data segments and a means for modifying the data segments with second data to generate modified data. The system further includes a means for scanning the system to determine available memory locations, a selector for selecting target memory locations within the available memory locations and a storage unit for storing the modified data at the target memory locations. A subset of the available memory locations are

located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located.

In the present invention as claimed in independent claim 126, a system for preventing unauthorized use of digital content data hosted on a system includes a modification unit for modifying the digital content data to generate modified data. The system further includes a means for determining whether an unauthorized attempt at accessing the digital content data occurs, and, in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter the unauthorized activity.

In the present invention as claimed in independent claim 155, a system for preventing unauthorized use of digital content data in a system having memory locations includes a scanner for scanning the system to determine available memory locations based on a file system identifying locations of files on the system, a means for selecting target memory locations within the available memory locations and a storage unit for storing the digital content data at the target memory locations. A subset of the available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located.

In the present invention as claimed in independent claim 180, a system for preventing unauthorized use of digital content data includes a subdividing unit for subdividing the digital content data into data segments, a modification unit for modifying the data segments with second data to generate modified data and a storage unit for storing the modified data at predetermined memory locations. The system further includes a scanner for scanning the system to determine available memory locations and a selector for selecting target memory locations within the available memory locations. The storage unit stores the modified data at the target memory locations and a subset of available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located.

Reitmeier, *et al.* discloses a secure information distribution system that includes a pixel domain encoder 105 (see Reitmeier, *et al.*, FIG. 1) which optionally imparts a digital watermarking to video information to produce an encoded information stream. A segmentation module 110 divides the encoded or un-encoded information stream into a plurality of segments to produce a segmented information stream. The segmented information stream is then transferred to a compression module 115A, which compresses the segmented information, and the segmented information stream is, optionally, stored in a first provider storage module 122. The compressed information stream is then transferred to a re-sequencing module 130. Re-sequencing module 130 rearranges the compressed information segments according to a predetermined, or pseudo-random, pattern. That is, re-sequencing module 130 shuffles the compressed and segmented information stream to produce a reordered or re-sequenced compressed information stream and an associated index table indicative of the re-sequencing operation performed. The index table includes pointers to the storage location of sequences ordered in their correct presentation sequence. The information stream is then transferred to encryption module 135 which scrambles the information stream. The index table may be distributed using a different medium than the re-ordered information. The re-ordered information may be distributed on a DVD-ROM, while the index table may be downloaded to a receiver/decoder from an on-line server. A second decryption module 160 decrypts the scrambled sequences. A random access module 165 utilizes the index table information to rearrange the de-scrambled sequences. Decrypted information stream segments are retrieved from a local storage module in a correct temporal or sequential order as indicated by the decrypted index table to produce a properly sequenced compressed information stream.

Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes “modifying the data segments with second data to generate modified data”, wherein “modifying the data segments” comprises “interleaving the data segments with the second data to generate interleaved data”, as claimed in independent claims 1, 161 and 167. The Office Action states at page 2, paragraph 2, that Reitmeier, *et al.* discloses encrypting the segments using common encryption techniques using a common encryption key,

which the Office Action analogizes to the claimed “interleaving the data segments with second data to generate interleaved data.” However, the applicants note that encryption and interleaving are independent processes. No necessary aspect of encryption requires interleaving. Encryption with an encryption key is not analogous to the claimed “interleaving the data segments with the second data.” Encryption processes transform data from its original form to a modified form. In encryption, the data in a modified form is only representative of the original data that has undergone a transformation; there is no second data in the modified, transformed data. In the present invention as claimed in claims 1, 161 and 167, encryption may also be optionally performed on the data, but this is a separate step from the step of interleaving. In interleaving, the original data is not “transformed” in the encryption sense; rather, the original data exists in its original state after interleaving. However, as a result of interleaving, second data is placed between elements of the first data. An example of this is provided in the specification as filed at least at page 16, lines 12-28. Interleaving creates data that are intelligible, i.e., can be executed as binary code, but are not accurate. Encryption, on the other hand, converts data to an unintelligible form, referred to as a “cipher” data. The encrypted cipher data, unlike interleaved data, cannot be executed as binary code. In contrast, the primary purpose of encryption is to create data that is unreadable/unuseable. While Reitmeier, *et al.* discloses an encryption process, encryption and interleaving are not the same, and are independent, distinct processes.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, “following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data”, as claimed in independent claims 1, 161 and 167. The Office Action states at pages 2-3, paragraph 3, that Reitmeier, *et al.* discloses decrypting the video segment, wherein the standard decryption involves using a decryption key. However, as discussed above, encryption and interleaving are distinct processes. Therefore, it follows that decryption and de-interleaving are also distinct processes.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in claim 29.

In the present application, as described in the specification as filed at least at page 24, line 9 through page 25, line 5, and page 28, line 14 through page 30, line 8, a table of contents or directory of a file system provides locations at which file system contents are stored. In the present invention as claimed, data can be stored at memory locations outside of the file system as defined by the table of contents on the same system as the file system and table of contents, i.e., not on an external device, but on the same system as the table of contents.

The Office Action states at page 3, paragraph 4, that Reitmeier, *et al.*, discloses storing the segments in first provider storage module 122 and indicates that the segmented information may be distributed on a DVD-ROM while the table is in the receiver/decoder from an online system. Reitmeier, *et al.* teaches that the re-ordered sequences and the index table can be distributed over different mediums, i.e., an external device. The different medium has its own table of contents that would define the location at which the index table is stored on the medium. The external devices of Reitmeier, *et al.*, i.e., the DVD-ROM or first provider storage module 122, do not store data outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located. Rather, if the memory locations are on the DVD-ROM or first provider storage module 122, the table of contents for the respective devices would define the locations of the available memory locations. There is no teaching or suggestion, in Reitmeier, *et al.*, of the re-ordered sequences being stored “outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located” as claimed in claim 29.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data hosted on a system that includes “determining whether an unauthorized attempt at accessing the digital content data occurs” and “in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity”, as claimed in independent claim 56. An example of this feature of the present invention is provided in the present application as filed, at least at page 38, lines 4-18, wherein a saturation profile is described as being a characterization of the normal system traffic. A saturation profile is created for the system, and, in the event of unauthorized access, the saturation profile of the system and system settings is read. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; there is no teaching or suggestion in Reitmeier, *et al.* of reading a saturation profile of a system or the generation of saturation traffic as claimed in claim 56.

In addition, Reitmeier, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent claim 85. Instead, as discussed above in connection with independent claim 29, Reitmeier, *et al.* teaches that the re-ordered sequences and the index table can be distributed over different mediums, i.e., an external device. The different medium has its own table of contents that would define the location at which the index table is stored on the medium. The external devices of Reitmeier, *et al.*, i.e., the DVD-ROM or first provider storage module 122, do not store data outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located. Rather, if the memory locations are on the DVD-ROM or first provider storage module 122, the table of contents for the respective devices would define the locations of the available memory locations. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored “outside the bounds of file system locations as identified by a

table of contents of the file system on which the subset of available memory locations are located” as claimed in claim 85.

Further, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes “a modification unit for modifying the data segments with second data to generate modified data”, the “modification unit modifying the data segments” comprising “interleaving the data segments with the second data to generate interleaved data”, as claimed in independent claims 89 and 175. As stated above in connection with independent claims 1, 161 and 167, the Office Action states at page 2, paragraph 2, that Reitmeier, *et al.* discloses encrypting the segments using common encryption techniques using a common encryption key, which the Office Action analogizes to the claimed “interleaving the data segments with second data to generate interleaved data.” However, the applicants note that encryption and interleaving are independent processes. No necessary aspect of encryption requires interleaving. Encryption with an encryption key is not analogous to the claimed “interleaving the data segments with the second data.” Encryption processes transform data from its original form to a modified form. In encryption, the data in a modified form is only representative of the original data that has undergone a transformation; there is no second data in the modified, transformed data. In the present invention as claimed in claims 89 and 175, encryption may also be optionally performed on the data, but this is a separate step from the step of interleaving. In interleaving, the original data is not “transformed” in the encryption sense; rather, the original data exists in its original state after interleaving. However, as a result of interleaving, second data is placed between elements of the first data. An example of this is provided in the specification as filed at least at page 16, lines 12-28. Interleaving creates data that are intelligible, i.e., can be executed as binary code, but are not accurate. Encryption, on the other hand, converts data to an unintelligible form, referred to as a “cipher” data. The encrypted cipher data, unlike interleaved data, cannot be executed as binary code. In contrast, the primary purpose of encryption is to create data that is unreadable/unuseable. While Reitmeier, *et al.* discloses an encryption process, encryption and interleaving are not the same, and are independent, distinct processes.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, “following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data”, as claimed in independent claims 89 and 175. As discussed above in connection with claims independent claims 1, 161 and 167, the Office Action states at pages 2-3, paragraph 3, that Reitmeier, *et al.* discloses decrypting the video segment, wherein the standard decryption involves using a decryption key. However, as discussed above, encryption and interleaving are distinct processes. Therefore, it follows that decryption and de-interleaving are also distinct processes.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of the available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents on which the subset of available memory locations are located”, as claimed in independent claim 115. Instead, as discussed above in connection with independent claims 29 and 85, Reitmeier, *et al.* teaches that the re-ordered sequences and the index table can be distributed over different mediums, i.e., an external device. The different medium has its own table of contents that would define the location at which the index table is stored on the medium. The external devices of Reitmeier, *et al.*, i.e., the DVD-ROM or first provider storage module 122, do not store data outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located. Rather, if the memory locations are on the DVD-ROM or first provider storage module 122, the table of contents for the respective devices would define the locations of the available memory locations. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored “outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located” as claimed in claim 115.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data hosted on a system that includes a “means for determining whether an unauthorized attempt at accessing the digital content data occurs” and “in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity”, as claimed in independent claim 126. An example of this feature of the present invention is provided in the present application as filed, at least at page 38, lines 4-18, wherein a saturation profile is described as being a characterization of the normal system traffic. A saturation profile is created for the system, and, in the event of unauthorized access, the saturation profile of the system and system settings is read. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; there is no teaching or suggestion in Reitmeier, *et al.* of reading a saturation profile of a system or the generation of saturation traffic as claimed in claim 126.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent claim 155. Instead, as discussed above in connection with independent claims 29, 85 and 115, Reitmeier, *et al.* teaches that the re-ordered sequences and the index table can be distributed over different mediums, i.e., an external device. The different medium has its own table of contents that would define the location at which the index table is stored on the medium. The external devices of Reitmeier, *et al.*, i.e., the DVD-ROM or first provider storage module 122, do not store data outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located. Rather, if the memory locations are on the DVD-ROM or first provider storage module 122, the table of contents for the respective devices would define the locations of the available memory locations. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored “outside the bounds of file system locations

as identified by a table of contents of the file system on which the subset of available memory locations are located” as claimed in claim 155.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes a “subset of available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent 180. Instead, as discussed above in connection with independent claims 29, 85, 115 and 155, Reitmeier, *et al.* teaches that the re-ordered sequences and the index table can be distributed over different mediums, i.e., an external device. The different medium has its own table of contents that would define the location at which the index table is stored on the medium. The external devices of Reitmeier, *et al.*, i.e., the DVD-ROM or first provider storage module 122, do not store data outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located. Rather, if the memory locations are on the DVD-ROM or first provider storage module 122, the table of contents for the respective devices would define the locations of the available memory locations. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored “outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located” as claimed in claim 180.

Weidong appears to disclose a method for managing encryption keys for data that includes generating a session key, encrypting the data using the session key and generating a key encryption key based on an initial vector. The initial vector is known only to a party encrypting the data and a party intended to decrypt the data. The session key is encrypted using the key encryption key.

Like Reitmeier, *et al.*, Weidong fails to teach or suggest a method of preventing unauthorized use of digital content data that includes “modifying the data segments with second data to generate modified data”, “modifying the data segments” comprising “interleaving the data

segments with the second data to generate interleaved data”, as claimed in independent claim 1. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest “modifying the data segments” with second data as claimed in claim 1. In addition, like Reitmeier, *et al.*, Weidong fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, “following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data”, as claimed in independent claim 1. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest “de-interleaving the data segments based on the second data” as claimed in claim 1.

Further, Weidong fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in claim 29.

In addition, like Reitmeier, *et al.*, Weidong fails to teach or suggest a system for preventing unauthorized use of digital content data that includes “a modification unit for modifying the data segments with second data to generate modified data”, the “modification unit modifying the data segments” comprising “interleaving the data segments with the second data to generate interleaved data”, as claimed in independent claim 89. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest “modifying the data segments” with second data. In addition, Weidong fails to teach or suggest a system for preventing unauthorized use of digital content data that includes “a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original data”, as claimed in independent claim 89. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest “de-interleaving the data segments based on the second data” as claimed in claim 89.

In addition, Weidong fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of the available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent claim 115.

Jensen, *et al.* is cited in the Office Action as teaching scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data. Jensen, *et al.* appears to disclose that information regarding locations of files is contained in a master file table.

Jensen, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes “modifying the data segments with second data to generate modified data”, “modifying the data segments” comprising “interleaving the data segments with the second data to generate interleaved data”, as claimed in independent claims 1, 161 and 167. In addition, Jensen, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, “following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data”, as claimed in independent claims 1, 161 and 167.

Jensen, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in claim 29. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

In addition, Jensen, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent claim 85. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes “a modification unit for modifying the data segments with second data to generate modified data”, the “modification unit modifying the data segments” comprising “interleaving the data segments with the second data to generate interleaved data”, as claimed in independent claims 89 and 175. In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes “a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original data”, as claimed in independent claims 89 and 175.

In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of the available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent claim 115. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

Further, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of the file system locations as identified

by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent claim 155. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes a “subset of available memory locations” that “are located outside the bounds of the file system locations as identified by a table of contents of the file system on which the subset of available memory locations are located”, as claimed in independent claim 180. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

Xu, *et al.* appears to disclose using obfuscation to prevent accurate disassembly of computer code. Assembly language instructions are used to confuse a disassembler.

Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes “modifying the data segments with second data to generate modified data”, “modifying the data segments” comprising “interleaving the data segments with the second data to generate interleaved data”, as claimed in independent claims 1 and 167. In addition, Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, “following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data”, as claimed in independent claims 1 and 167.

In addition, Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes “a subset of available memory locations” that “are located outside the bounds of file system locations as identified by a

table of contents of the file system on which the subset of available memory locations are located”, as claimed in claim 29.

In addition, like Reitmeier, *et al.*, Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data hosted on a system that includes “determining whether an unauthorized attempt at accessing the digital content data occurs” and “in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity”, as claimed in independent claim 56. The Office Action states, at page 3, section 5, that Xu, *et al.* discloses inserting an obfuscation instruction or causing a disassembler to not disassemble the bytes subsequent to the obfuscating instruction, and inserting a branch instruction to invoke execution of the bytes subsequent to the obfuscating instructions. However, there is no teaching or suggestion in Xu, *et al.* of “reading a saturation profile of the system and system settings” as claimed in claim 56. An example of this feature of the present invention is provided in the present application as filed, at least at page 38, lines 4-18, wherein a saturation profile is described as being a characterization of the normal system traffic. A saturation profile is created for the system, and, in the event of unauthorized access, the saturation profile of the system and system settings is read. Xu, *et al.* in no way teaches or suggests creating a saturation profile of the system and system settings and subsequently reading the saturation profile. Rather, Xu, *et al.* merely discloses means of obfuscating or confusing a disassembler. In addition, Xu, *et al.* fails to teach or suggest generating “saturation traffic on the system” as claimed. Instead, Xu, *et al.* discloses the insertion of single instructions into code. In the present application, as described in the specification as filed at least at page 37, line 20 through page 39, line 2, the saturation traffic is created in such volume that monitoring/logging/data watching debug techniques are easily overwhelmed such that the events of interest to one debugging or reverse engineering the system are therefore lost in the process. In Xu, *et al.*, the obfuscating instructions do not overwhelm the disassembler.

In addition, Xu, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes “a modification unit for modifying the data segments with

second data to generate modified data”, the “modification unit modifying the data segments” comprising “interleaving the data segments with the second data to generate interleaved data”, as claimed in independent claims 89 and 175. In addition, Xu, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes “a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original data”, as claimed in independent claims 89 and 175.

In addition, Xu, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data hosted on a system that includes a “means for determining whether an unauthorized attempt at accessing the digital content data occurs” and “in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity”, as claimed in independent claim 126. As discussed in connection with independent claim 56, an example of this feature of the present invention is provided in the present application as filed, at least at page 38, lines 4-18, wherein a saturation profile is described as being a characterization of the normal system traffic. A saturation profile is created for the system, and, in the event of unauthorized access, the saturation profile of the system and system settings is read. Xu, *et al.* in no way teaches or suggests creating a saturation profile of the system and system settings and subsequently reading the saturation profile. Rather, Xu, *et al.* merely discloses means of obfuscating or confusing a disassembler. In addition, Xu, *et al.* fails to teach or suggest generating “saturation traffic on the system” as claimed. Instead, Xu, *et al.* discloses the insertion of single instructions into code. In the present application, as described in the specification as filed at least at page 37, line 20 through page 39, line 2, the saturation traffic is created in such volume that monitoring/logging/data watching debug techniques are easily overwhelmed such that the events of interest to one debugging or reverse engineering the system are therefore lost in the process. In Xu, *et al.*, the obfuscating instructions do not overwhelm the disassembler.

Atallah, *et al.* is cited in the Office Action as disclosing that determining whether an unauthorized attempt at accessing the digital content data occurs comprises monitoring activity of the system hosting the digital content data and determining whether the activity is inconsistent with the type of digital content data being hosted.

Atallah, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data hosted on a system that includes “determining whether an unauthorized attempt at accessing the digital content data occurs” and “in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity”, as claimed in independent claim 56.

In addition, Atallah, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data hosted on a system that includes a “means for determining whether an unauthorized attempt at accessing the digital content data occurs” and “in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity”, as claimed in independent claim 126.

CONCLUSION

Since none of Reitmeier, *et al.*, Weidong, Jensen, *et al.*, Xu, *et al.* teach or suggest the limitations of independent claims 1, 29 and 89, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 1 and 89 under 35 U.S.C. 102(e) as being anticipated by Reitmeier, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 2-5, 11-14, 26, 90-92, 98-101 and 112, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 15-19, 21-24, 102-106 and 108-110 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.*, it follows that these claims should inherit the allowability of the

independent claims from which they depend. With regard to the rejections of dependent claims 27, 28, 113 and 114 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 186-188 and 191-193 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Wiedong, it follows that these claims should inherit the allowability of the independent claims from which they depend. Reconsideration of the rejection of independent claims 29, 85, 115, 155, 161 and 180 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 30, 32-39, 43-53, 86-87, 116, 118-121, 123-125, 156-157, 162-166 and 181-183, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 40, 41, 42 and 122 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Weidong, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 54 and 55 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Xu, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend.

Further, since none of Reitmeier, *et al.*, Jensen, *et al.* and Xu, *et al.* teach or suggest the limitations of independent claims 167 and 175, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 167 and 175 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* and Xu, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 168-171 and 176, it follows that this claim should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 172-174 and 177-179 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Jensen, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend.

Further, since none of Reitmeier, *et al.*, Xu, *et al.* and Atallah, *et al.* teaches or suggests the limitations of independent claims 56 and 126, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 56 and 126 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* and Xu, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 57, 59-63, 127, 129, 130, 132 and 133, it follows that this claim should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 131 and 61 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Atallah, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend.

Closing Remarks

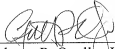
In view of the amendments to the claims and the foregoing remarks, it is believed that, upon entry of this Amendment, all claims pending in the application will be in condition for allowance. Therefore, it is requested that this Amendment be entered and that the case be allowed and passed to issue. If a telephone conference will expedite prosecution of the application, the Examiner is invited to telephone the undersigned.

Authorization is hereby given to charge Deposit Account No. 50-1798 for any additional fees which may be due or to credit any overpayment.

Respectfully submitted,

Date: January 14, 2008
MILLS & ONELLO LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900
Facsimile: (617) 742-7774

J:\ECD\0012\AA\Amendment\afterfinal.wpd



Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant